PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250192
(43)Date of publication of application : 17.09.1999

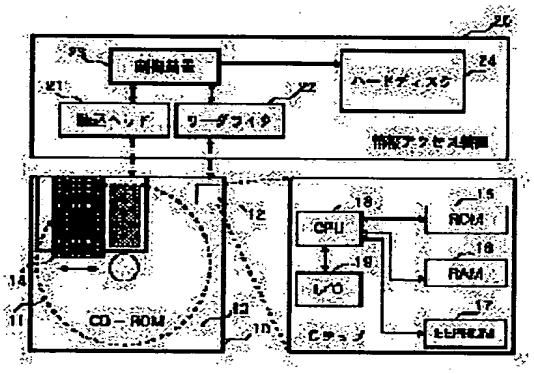
(51)Int.Cl. G06K 17/00
G06F 9/06
G06F 12/14
G11B 7/24
G11B 19/04

(21)Application number : 10-050713
(22)Date of filing : 03.03.1998

(71)Applicant : NTT DATA CORP
(72)Inventor : ICHIHARA NAOHISA
OKUMA YOSHIYUKI

(54) RECORDING MEDIUM WITH BUILT-IN IC CHIP AND INFORMATION ACCESS CONTROLLER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a recording medium provided with a built-in IC chip and capable of holding security for digital information such as software to be recorded.
SOLUTION: The recording medium 10 is constituted of housing a recording medium 11 such as a CD-ROM in a casing 13 having a shape to be housed in an information access device 20 and fitting an IC chip 12 to a prescribed position of the casing 13. A ciphered file obtained by ciphering digital information is recorded in the recording medium 11. At the time of accessing information by the device 20, the IC chip 12 executes verification, and when the verified result is affirmative, sends a decipher key for deciphering the ciphered file to the device 20. The device 20 receives the decipher key from the IC chip 12, deciphers the ciphered file and installs the deciphered file.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－250192

(43)公開日　平成11年(1999)９月17日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｂ
					Ｅ
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｌ
					５５０Ａ
	12/14	３２０		12/14	３２０Ｆ

審査請求　未請求　請求項の数10　ＯＬ　（全７頁）　最終頁に続く

(21)出願番号　特願平10－50713

(22)出願日　平成10年(1998)３月３日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号

(72)発明者　市原　尚久
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

(72)発明者　大熊　善之
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内

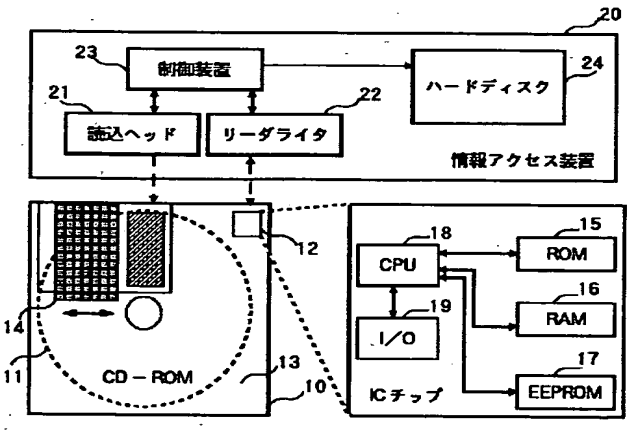
(74)代理人　弁理士　鈴木　正剛

(54)【発明の名称】　ＩＣチップ内蔵記録媒体、情報アクセス制御装置

(57)【要約】

【課題】　記録されるソフトウェア等のデジタル情報に対するセキュリティを確保できるＩＣチップ内蔵記録媒体を提供する。

【解決手段】　本発明のＩＣチップ内蔵記録媒体１０は、情報アクセス装置２０に収容可能な形状の筐体１３の内部にＣＤ－ＲＯＭ等の記録媒体１１を収容するとともに筐体１３の所定部位にＩＣチップ１２を取り付けて構成される。記録媒体１１には、デジタル情報を暗号化した暗号化ファイルを記録しておく。ＩＣチップ１２は、情報アクセス装置２０による情報アクセスの際に認証を行い、肯定的であった場合は、上記暗号化ファイルを復号化させるための復号鍵を情報アクセス装置２０に送る。情報アクセス装置２０は、ＩＣチップ１２から復号鍵を受け取って暗号化ファイルを復号し、インストールを行う。



1

【特許請求の範囲】

【請求項１】　記録媒体に記録されたデジタル情報の読み取り及びＩＣチップへの情報アクセスとを行う装置に収容可能な形状の筐体を有し、
該筐体の内部には前記記録媒体が収容され、該筐体の所定部位には前記ＩＣチップが取り付けられており、
前記ＩＣチップが、前記装置による前記デジタル情報の読み取りを規制するように構成されていることを特徴とする、ＩＣチップ内蔵記録媒体。

【請求項２】　前記デジタル情報が暗号化されたデジタル情報であり、
前記ＩＣチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記復号鍵を渡して前記暗号化されたデジタル情報を復号化させるアクセス制御手段を備えていることを特徴とする請求項１記載のＩＣチップ内蔵記録媒体。

【請求項３】　前記デジタル情報が実行形式のプログラムであり、
前記ＩＣチップは、前記実行形式のプログラムの実行に必要な条件情報を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記条件情報を渡して前記実行形式のプログラムの実行状態を形成させるアクセス制御手段を備えていることを特徴とする請求項１記載のＩＣチップ内蔵記録媒体。

【請求項４】　前記アクセス制御手段は、前記情報アクセスの際に受信した乱数データの正当性を確認することにより前記認証を行うように構成されていることを特徴とする請求項２または３記載のＩＣチップ内蔵記録媒体。

【請求項５】　コンピュータ装置が読み取り可能なインストーラ及びインストール対象となるデジタル情報を記録した記録媒体を前記コンピュータ装置に収容可能な形状の筐体に収容するとともに、該筐体の所定部位に、指令入力を契機に認証を行い、認証結果を出力するＩＣチップを備えたＩＣチップ内蔵記録媒体であって、
前記インストーラが、
前記ＩＣチップに所定の認証データに基づく認証指令を送出するとともに当該ＩＣチップから前記認証結果を取得し、認証結果が肯定的の場合に前記ＩＣチップに記録された前記デジタル情報をインストールする処理を前記コンピュータ装置に実行させるものであることを特徴とするＩＣチップ内蔵記録媒体。

【請求項６】　前記デジタル情報が暗号化されたデジタル情報であり、
前記ＩＣチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の

2

場合に前記復号鍵を渡すように構成されており、
前記インストーラは、前記暗号化されたデジタル情報を前記復号鍵で復号化しインストールする処理を前記コンピュータ装置に実行させるものであることを特徴とする請求項５記載のＩＣチップ内蔵記録媒体。

【請求項７】　前記ＩＣチップは、前記認証指令の入力を契機に参照鍵を生成する鍵生成手段と、生成された参照鍵と前記復号鍵とを照合する照合手段とを備え、両鍵が合致したときに肯定的な認証結果を出力することを特徴とする請求項２または６記載のＩＣチップ内蔵記録媒体。

【請求項８】　前記ＩＣチップは、前記インストールの回数を計数するインストール回数計数手段と、該インストール回数計数手段による計数値が所定値を越えたときに前記インストールを制限する手段とを備えていることを特徴とする請求項６記載のＩＣチップ内蔵記録媒体。

【請求項９】　デジタル情報及びこのデジタル情報のインストーラを記録した記録媒体を筐体内に収容するとともに、該筐体の所定部位にＩＣチップが固定されたＩＣチップ内蔵記録媒体への情報アクセスを行う装置であって、
前記筐体の収容時に前記ＩＣチップとの間で情報の授受を行うリーダライタと、
前記リーダライタを通じて前記ＩＣチップに認証指令を送出するとともに該ＩＣチップからの認証結果が肯定的の場合に前記記録媒体から前記インストーラを読み込んで前記デジタル情報をインストールする制御手段とを有することを特徴とする情報アクセス装置。

【請求項１０】　前記記録媒体には暗号化されたデジタル情報が記録され、前記ＩＣチップには前記暗号化されたデジタル情報を復号化する復号鍵が保持されており、前記制御手段は、前記認証結果が肯定的の場合に前記ＩＣチップに格納された復号鍵を用いて前記暗号化されたデジタル情報を復号化した後に前記インストールを行うように構成されていることを特徴とする請求項９記載の情報アクセス装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、コンピュータプログラムを記録するためのパッケージ型の記録媒体、例えばフレキシブルディスク（ＦＤ）、コンパクトディスク型ＲＯＭ（ＣＤ－ＲＯＭ）、光磁気ディスク（ＭＯディスク）、ミニディスク（ＭＤ）と、これらの記録媒体へのアクセスを行うアクセス装置に関し、特に、記録媒体に記録されるコンピュータプログラムのセキュリティを確保する手法に関する。

【０００２】

【従来の技術】コンピュータプログラムやデータ、コンテンツ等のデジタル情報を流通させる場合、これらをコンピュータ読み取り可能な形態でパッケージ型の記録媒

体に記録することがよく行われている。ユーザは、この記録媒体をコンピュータ装置にセットし、インストールして使用できるようにする。しかし、従来、記録媒体には記録情報のセキュリティ対策が十分に施されていないため、不正コピーを防ぐための対策は貧弱である。

【０００３】例えば購入者から記録媒体を借用した第三者が、デジタル情報を自分のコンピュータ装置へインストールすることはきわめて容易である。ソフトウエアＩＤ番号付与やユーザ登録制なども試みられているが、不正コピー防止の根本的な解決には結びつかないのが現状である。なお、記録情報の同一性を保持する手段として、例えばＦＤの場合には、パッケージのスライドスイッチを「書き込み不可」に設定することはよく行われることであるが、この「書き込み不可」の状態を「書き込み可能」の状態に変更することは極めて容易であり、セキュリティと呼ぶには至らない。

【０００４】

【発明が解決しようとする課題】近年、記録対象となるデジタル情報のサイズは肥大化しており、それに対応して、記録媒体も、ＣＤ－ＲＯＭのような、読み取り専用ではあるが、大容量の記録媒体が使用されている。しかし、このような記録媒体は、製造工程の都合上、媒体毎のソフトウエアＩＤ番号の付与は行われていない。通常、プログラム等のインストールの際には、ソフトウエアＩＤ番号を入力することが必要となるが、多くの場合、このソフトウエアＩＤ番号が記録媒体に記録されているわけではなく、ソフトウエアＩＤ番号をハッシュ関数にかけた結果が予め記録媒体内に保存されたテーブルにあれば、インストールできるようになっている。例えばＡ氏の購入した記録媒体のソフトウエアＩＤ番号で、Ｂ氏の購入した同じ記録媒体の記録情報のインストールが可能となる。このように同じ記録媒体から何度でもインストールできる事態は好ましくなく、デジタル情報のセキュリティを図るための技術開発が望まれていた。

【０００５】そこで本発明は、ＩＣチップの耐タンパ性と高セキュリティ性とを利用して、記録されたデジタル情報のセキュリティを確保するＩＣチップ内蔵記録媒体を提供することを課題とする。本発明の他の課題は、ＩＣチップ内蔵記録媒体への情報アクセスを行う情報アクセス装置を提供することにある。

【０００６】

【課題を解決するための手段】上記課題を解決する本発明のＩＣチップ内蔵記録媒体は、記録媒体に記録されたデジタル情報の読み取り及びＩＣチップへの情報アクセスとを行う装置に収容可能な形状の筐体を有するもので、該筐体の内部には前記記録媒体が収容され、所定部位には前記ＩＣチップが取り付けられており、前記ＩＣチップは、前記装置による前記デジタル情報の読み取りを規制するように構成されていることを特徴とする。

【０００７】前記デジタル情報は、例えば所定の暗号アルゴリズムで暗号化されたデジタル情報とする。この場合、前記ＩＣチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記復号鍵を渡して前記暗号化されたデジタル情報を復号化させるアクセス制御手段を備えるようにする。

【０００８】前記デジタル情報は、実行形式のプログラムであってもよい。この場合、前記ＩＣチップは、前記実行形式のプログラムの実行に必要な条件情報を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記条件情報を渡して前記実行形式のプログラムの実行状態を形成させるアクセス制御手段を備えるようにする。条件情報は、例えば起動情報、鍵情報、あるいはプログラムの実行手順を定めたデータである。

【０００９】前記アクセス制御手段は、例えば、前記情報アクセスの際に受信した乱数データの正当性を確認することにより前記認証を行うように構成される。

【００１０】本発明の他のＩＣチップ内蔵記録媒体は、コンピュータ装置が読み取り可能なインストーラ及びインストール対象となるデジタル情報を記録した記録媒体を前記コンピュータ装置に収容可能な形状の筐体に収容したものである。該筐体の所定部位には、指令入力を契機に認証を行い、認証結果を出力するＩＣチップを備えている。前記インストーラは、前記ＩＣチップに所定の認証データに基づく認証指令を送出するとともに当該ＩＣチップから前記認証結果を取得し、認証結果が肯定的の場合に前記ＩＣチップに記録された前記デジタル情報をインストールする処理を前記コンピュータ装置に実行させるものである。

【００１１】このようなＩＣチップ内蔵記録媒体において、前記デジタル情報は暗号化されたデジタル情報であってもよい。この場合、前記ＩＣチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に前記復号鍵を渡すように構成し、前記インストーラは、前記暗号化されたデジタル情報を前記復号鍵で復号化してインストールする処理を前記コンピュータ装置に実行させるようにする。

【００１２】なお、前記ＩＣチップが復号鍵を保持する場合は、前記認証指令の入力を契機に参照鍵を生成する鍵生成手段と、生成された参照鍵と前記復号鍵とを照合する照合手段とをさらに備え、両鍵が合致したときに肯定的な認証結果を出力するように構成する。

【００１３】好ましくは、前記ＩＣチップが、さらに、前記インストールの回数を計数するインストール回数計数手段と、該インストール回数計数手段による計数値が所定値を越えたときに前記インストールを制限する手段とを備えるようにする。

【００１４】上記他の課題を解決する本発明の情報アクセス装置は、デジタル情報及びこのデジタル情報のインストーラを記録した記録媒体を筐体内に収容するとともに、該筐体の所定部位にＩＣチップが固定されたＩＣチップ内蔵記録媒体への情報アクセスを行う装置であって、前記筐体の収容時に前記ＩＣチップとの間で情報の授受を行うリーダライタと、前記リーダライタを通じて前記ＩＣチップに認証指令を送出するとともに該ＩＣチップからの認証結果が肯定的の場合に前記記録媒体から前記インストーラを読み込んで前記デジタル情報をインストールする制御手段とを有することを特徴とする。

【００１５】前記記録媒体に暗号化されたデジタル情報が記録され、前記ＩＣチップに前記暗号化されたデジタル情報を復号化する復号鍵が保持されている場合、前記制御手段は、前記認証結果が肯定的の場合に前記ＩＣチップに格納された復号鍵を用いて前記暗号化されたデジタル情報を復号化した後に前記インストールを行うように構成する。

【００１６】

【発明の実施の形態】以下、本発明のＩＣチップ内蔵記録媒体と、本発明の情報アクセス装置とを備えて構成されるコンピュータシステムの実施の形態を説明する。ここでは、デジタル情報を記録する記録媒体をＣＤ－ＲＯＭとし、デジタル情報は所定の暗号アルゴリズムで暗号化されているものとする。以下、平文のデジタル情報を単にファイル、暗号化されたファイルを暗号化ファイルと称する。

【００１７】図１は、本実施形態によるコンピュータシステムの構成図である。このコンピュータシステムは、ＩＣチップ１２を有するＩＣチップ内蔵ＣＤ－ＲＯＭ（以下、ＩＣ－ＣＤ）１０と、ＩＣ－ＣＤ１０のＣＤ－ＲＯＭ１１に記録されたファイルまたは暗号化ファイルをインストールするための情報アクセス装置２０とを備えて構成される。

【００１８】情報アクセス装置２０は、ＣＤ－ＲＯＭ１１に記録された情報の読込を行う読込ヘッド２１と、ＩＣチップ１２との間で情報の授受を行うリーダライタ２２とを備え、さらに、装置内部のＣＰＵ（図示省略）が所定の制御プログラムを読み込むことにより実現される制御装置２３と、補助記憶装置である大容量のハードディスク２４とを少なくとも有する。通常、この情報アクセス装置２０は、パーソナルコンピュータやワークステーションで実現される。

【００１９】ＩＣ－ＣＤ１０は、情報アクセス装置２０のメディア装着機構（図示省略）に装着可能な形状、寸法の樹脂製の筐体１３内にＣＤ－ＲＯＭ１１を収容するとともに、筐体１３の所定部位、すなわちにリーダライタ２２に対応する筐体正面部にＩＣチップ１２を取り付けたものである。筐体１３には、スライド自在のカバー１４が取り付けられ、ＩＣ－ＣＤ１０がメディア装着機構に装着されたときに、カバー１４がスライドしてＣＤ－ＲＯＭ１１の記録面が露出し、読込ヘッド２１がＣＤ－ＲＯＭ１１の記録情報を読み込めるようになっている。

【００２０】ＩＣチップ１２には、少なくともＲＯＭ１５、ＲＡＭ１６、ＥＥＰＲＯＭ１７、ＣＰＵ１８、Ｉ／Ｏポート１９が形成されている。

【００２１】ＲＯＭ１５には、ＣＰＵ１８によって読み取られて実行されるＩＣ用プログラムが格納されている。ＲＡＭ１６はＣＰＵ１８によって使用される作業領域であり、ＥＥＰＲＯＭ１７には、鍵格納領域１７１、インストール回数格納領域１７２、鍵生成関数格納領域１７３が形成されている。ＣＰＵ１８は、関数演算や入出力制御を行う論理演算プロセッサである。Ｉ／Ｏポート１９は、リーダライタ２２との間の情報の入出力ポートである。

【００２２】本実施形態では、ＣＤ－ＲＯＭ１１に、上記暗号化ファイルのほかに、暗号アルゴリズムの情報、インストーラを記録しておく。情報アクセス装置２０の側では、ＩＣ－ＣＤ１０がメディア装着機構に装着されたときに、ＣＤ－ＲＯＭ１１に記録されたインストーラを読み込み、ＣＰＵがそれを実行することにより、種々の機能ブロックを装置内に形成する。ＩＣチップ１２においても、ＣＰＵ１８がＩＣ用プログラムを読み込んで実行することにより、種々の機能ブロックを形成する。

【００２３】図２は、これらの機能ブロックの相関図である。すなわち、情報アクセス装置２０には、乱数処理部２６、復号部２７、メモリ制御部２８の機能ブロックを形成する。乱数処理部２６は、図示しない入力装置を通じてユーザの認証データ（乱数）を受け付け、これをリーダライタ２２を通してＩＣチップ１２に出力するものである。復号部２７は、ＩＣチップ１２から復号鍵が送られたときにＣＤ－ＲＯＭ１１に記録された暗号化ファイルを復号するものである。メモリ制御部２８は、復号化されたファイルをハードディスク２４に格納するための制御を行うものである。

【００２４】一方、ＩＣチップ１２には、メモリ制御部１２１、鍵生成部１２２、照合部１２３、回数検出部１２４の機能ブロックを形成する。メモリ制御部１２１は、ＥＥＰＲＯＭ１７内の情報の記録制御及び再生制御を行うものであり、鍵生成部１２２は、上記乱数処理部２６から入力される乱数に基づいて参照鍵を生成するものである。照合部１２３は、鍵生成部１２２で生成された参照鍵がＥＥＰＲＯＭ１７内の鍵格納領域１７１に格納されている鍵と合致するかどうかを照合し、この照合結果と、インストール回数格納領域１７２に格納されたインストール可能回数を参照してインストールの可否をリーダライタ２２を通じて復号部２７に出力するものである。回数検出部１２４は、インストール回数格納領域１７２内のインストール回数を更新するものである。

【００２５】ＩＣ－ＣＤ１０に記録される暗号化ファイルは、例えば公知の共通鍵方式で暗号化される。この場合の暗号化処理の手順を示したのが図３である。まず、ＣＤ－ＲＯＭ１０にファイルを記録する記録装置（図示省略）において、乱数を発生させ（ステップＳ１０１）、この乱数と鍵生成関数とを用いて、暗号鍵を生成する（ステップＳ１０２）。例えば、鍵生成関数をＧ（ｘ）、乱数をＲとすると、暗号鍵Ｋは、下記（１）式で求められる。Ｋ＝Ｇ（Ｒ）…（１）

【００２６】次に、暗号鍵Ｋと共通暗号アルゴリズムＣとを用いて、対象となるファイルＦ０を暗号化する。これにより生成される暗号化ファイルＦ１は、下記（２）式により求めることができる（ステップＳ１０３）。

Ｆ１＝Ｃ（Ｆ０）…（２）

【００２７】記録装置は、このようにして生成された暗号化ファイルＦ１を、共通暗号アルゴリズムＣ、インストーラと共にＣＤ－ＲＯＭ１１に記録する。また、ＩＣチップ１２の鍵格納領域１７１、インストール回数格納領域１７２、鍵生成関数格納領域１７３に、それぞれ暗号鍵Ｋ、インストール可能回数の初期値、鍵生成関数Ｇ（ｘ）を記録する。ユーザに対しては、ＩＣ－ＣＤ１０と暗号鍵Ｋの生成に用いられた乱数Ｒとを配送する。

【００２８】次に、コンピュータシステムにおいて、ユーザが、ＩＣ－ＣＤ１０に記録された暗号化ファイルＦ１を情報アクセス装置２０にインストールする場合の手順を、図４に従って説明する。

【００２９】乱数ＲとＩＣ－ＣＤ１０とを受け取ったユーザがメディア装着機構にＩＣ－ＣＤ１０を装着すると、情報アクセス装置２０は、ＣＤ－ＲＯＭ１１に記録されたインストーラを読み込んで実行する（ステップＳ２０１）。その後、乱数処理部２６でユーザからの乱数Ｒの入力を受け付け、これを認証指令として、ＩＣチップ１２の鍵生成部１２２に出力する（ステップＳ２０２）。鍵生成部１２２は、ＥＥＰＲＯＭ１７の鍵生成関数格納領域１７３に格納されている鍵生成関数Ｇ（ｘ）をメモリ制御部１２１を介して受け取り、参照鍵を生成する（ステップＳ２０３）。

【００３０】照合部１２３は、インストール回数格納領域１７２に格納されているインストール可能回数Ｎが“１”以上であり、且つ、鍵格納領域１７１に予め格納されている鍵と鍵生成部１２２で生成した参照鍵とを照合する（ステップＳ２０４）。両者が合致する場合は（ステップＳ２０４；Ｙｅｓ）、回数検出部１２４に対して肯定的な認証結果、すなわち「ＯＫ判定」を送信するとともに、復号部２７に対してこの「ＯＫ判定」と復号鍵とを送信する。

【００３１】回数検出部１２４は、インストール可能回数Ｎを“Ｎ－１”に更新するとともに、これをメモリ制御部１２１を介してインストール回数格納領域１７２に格納する（更新する）（ステップＳ２０５）。

【００３２】情報アクセス装置２０では、復号部２７において、復号鍵と共通暗号アルゴリズムＣに基づいて暗号化ファイルＦ１を復号化し、これをメモリ制御部２８に出力する（ステップＳ２０６）。メモリ制御部２８は、復号化後のファイルをハードディスク２４にインストールし（ステップＳ２０７）、処理を終了させる。一方、ステップＳ２０４において、参照鍵と復号鍵が合致しなかった場合、あるいはインストール可能回数Ｎが“０”であった場合（ステップＳ２０４；Ｎｏ）、照合部１２３は、復号部２７に否定的な認証結果、すなわち「ＮＧ判定」を送信する。このＮＧ判定を受信した復号部２７は、直ちに処理を終了させる。

【００３３】このように、暗号化ファイルＦ１をＣＤ－ＲＯＭ１１に記録し、復号鍵等をＩＣチップ１２に保持させることにより、ＣＤ－ＲＯＭ１１に記録された情報のアクセス制御をＩＣチップ１２に任せることが可能になる。例えば、従来のＣＤ－ＲＯＭやＦＤ等では不可能であった、ユーザの正当性の認証やインストール回数の制限を行うことが可能になり、ファイルのセキュリティ対策が万全となる。

【００３４】なお、本実施形態では、記録媒体として、筐体１３に格納されたいわゆるパッケージ型のＣＤ－ＲＯＭを例に挙げて説明したが、ＩＣチップを固定できる構造の他の記録媒体、例えばＭＯやＤＶＤ等にも同様に本発明を適用できるものである。

【００３５】

【実施例】次に、上記ＩＣ－ＩＤ１０の実施例を説明する。

（第１実施例）上記ＩＣ－ＩＤ１０を用いることにより、アプリケーション処理の分散化を行うことが可能である。つまり、所定のアプリケーション処理を実行するためのファイルのうち、実行形式のプログラムの部分だけをＣＤ－ＲＯＭ１１に記録してインストールの対象ファイルとし、ＩＣチップ１２には上記プログラム用のバッチ・モジュール等を搭載し、両者を組み合わせて一つのアプリケーション処理を実行できるようにすることも可能である。このように、アプリケーション処理の分散化を行うことにより、インストール時のメモリ容量を低減させることができるようになる。

【００３６】（第２実施例）また、ＣＤ－ＲＯＭ１１に実行形式のプログラムを記録するとともに、ＩＣチップ１２（ＥＥＰＲＯＭ１７）にそのプログラムの実行に必要な条件情報を更新自在に記録できるようにし、これらを情報アクセス装置２０において合体させることで、必ずしもインストールすることなく、ＩＣ－ＣＤ１０のみで上記プログラムを実行できるようにする形態も可能である。

【００３７】この場合の実行形式のプログラムの例としては、例えばＲＰＧ（ロールプレイングゲーム）等のゲームプログラム、ビジネス用ＡＰ（ＡＰは、アプリケー

ション・プログラム、以下同じ）、電子マネー用ＡＰ等が挙げられる。また、ＩＣチップ１２に記録される条件情報としては、ゲームプログラムの場合はプレイヤ毎のゲーム進行情報その他の可変情報、ビジネス用ＡＰの場合はデータ、電子マネー用ＡＰの場合は電子マネー情報となる。各プログラムの起動に必要なコンピュータ装置の環境情報や鍵情報としてもよい。

【００３８】このような使用形態を採用することにより、実行形式のプログラムと一緒に条件情報を持ち歩き、プログラム実行時に両者を合体させてＩＣ－ＣＤ１０上から起動させることができるので、複数のプログラムの実行環境の競合を防止できるようになる。

【００３９】情報アクセス装置２０にインストールする必要がある場合でも、プログラムとその条件情報とが一体化されているので、ＡＰと条件情報とを別々にコンピュータ装置に移動させる必要が無くなるので、プログラムの実行環境の形成の便宜を図ることができる。

【００４０】

【発明の効果】以上の説明から明らかなように、本発明のＩＣチップ内蔵記録媒体によれば、記録されたデジタル情報や、デジタル情報の配送時のセキュリティが万全となり、不正コピーの防止のみならず、ライセンスパック契約等をソフトウェアメーカの関与なしに行うことが可能になる、という特有の効果が得られる。

【図面の簡単な説明】

【図１】本発明を適用したコンピュータシステムの一実施の形態を示す構成図。

＊【図２】本実施形態による機能ブロックの相関図。

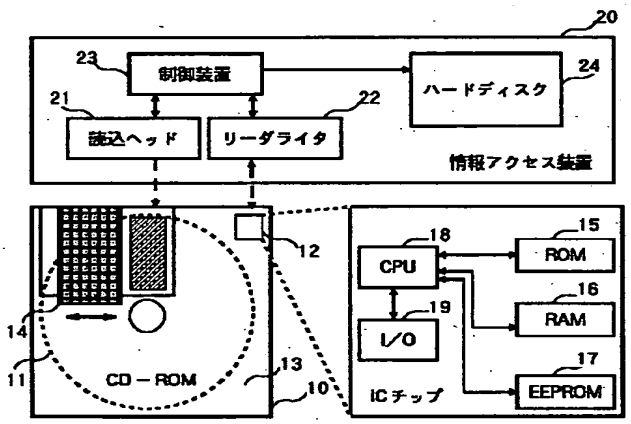
【図３】本実施形態による記録対象ファイルの暗号化手順を示した説明図。

【図４】本実施形態による記録対象ファイルのインストールの手順説明図。

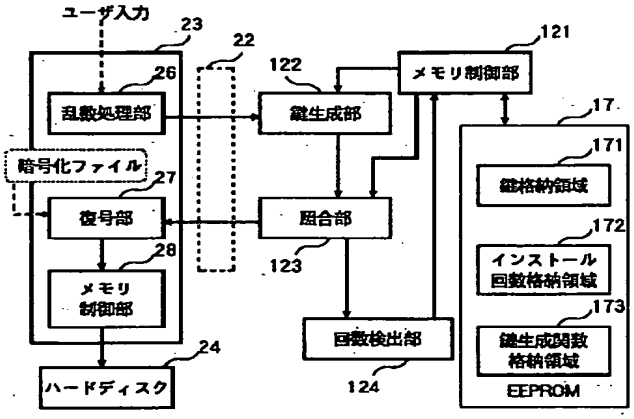
【符号の説明】

１０　ＩＣ－ＣＤ
１１　ＣＤ－ＲＯＭ
１２　ＩＣチップ
１３　筐体
１４　カバー
１７　ＥＥＰＲＯＭ
１８　ＣＰＵ
２０　情報アクセス装置
２１　読込ヘッド
２２　リーダライタ
２３　制御装置
２４　ハードディスク
２６　乱数処理部
２７　復号部
２８，１２１　メモリ制御部
１２２　鍵生成部
１２３　照合部
１２４　回数検出部
１７１　鍵格納領域
１７２　インストール回数格納領域
＊　１７３　鍵生成関数格納領域

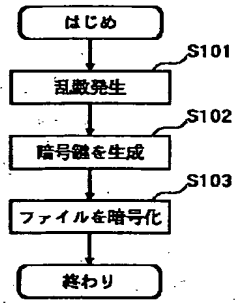
【図１】



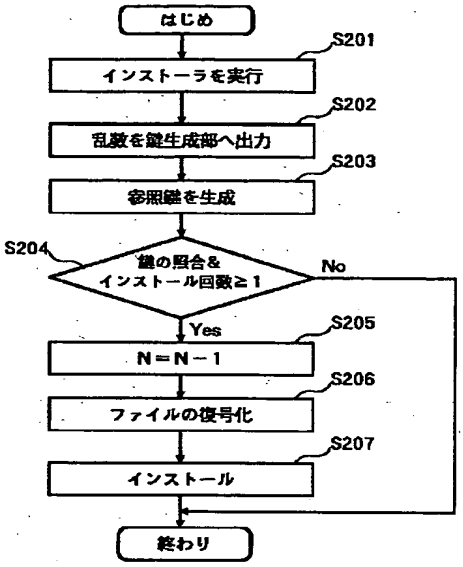
【図２】



【図３】



【図４】



フロントページの続き

(51) Int. Cl.[6]		識別記号	FI		
G０６F	12/14	３２０	G０６F	12/14	３２０E
G１１B	7/24	５７１	G１１B	7/24	５７１A
					５７１Z
	19/04	５０１		19/04	５０１H